USAREUR Bulletin

HQ USAREUR/7A
Unit 29351
APO AE 09014

USAREUR Bulletin Number 4
15 February 2001

This bulletin expires 1 year from date of publication.

CONTENTS

USAREUR Information Assurance Policy

The integrity of USAREUR automation systems must be preserved. Information assurance (IA) protects automation systems and data, whether installed on or passed through the system. Safeguarding both systems and data is a nonnegotiable responsibility.

Appendix A provides the IA policy for USAREUR. This policy supersedes all previously published IA

policy.

Black History Month

Black History Month will be celebrated during the month of February. The theme of this year's observance is "Creating and Defining the African American Community: Family, Church, Politics, Culture."

Commemorative events will be conducted throughout USAREUR to mark this observance. *The HQ USAREUR/7A Equal Opportunity Office Website* provides information on these events. Leaders should refer to USAREUR Pamphlet 600-21 and encourage participation in these events within mission constraints.

FormFlow Filler Software

Army personnel may now download FormFlow filler software free of charge from the Internet at *http://pmscp.monmouth.army.mil/jetform/jetform.htm*. Using the Army-wide site license will standardize the use of filler software throughout USAREUR.

The United States Army Publications Distribution Center, Europe, will no longer stock forms that are available in electronic media, except for high-use forms that would not be cost-effective to print individually.

FormFlow filler software is also on the 1 January 2001 edition of EM 0001 (Army Electronic Library). EM 0001 may be ordered through normal publications channels.

ODCSIM Reorganization

The Office of the Deputy Chief of Staff, Information Management (ODCSIM), HQ USAREUR/7A, will be reorganized on 19 February 2001. The new organizational structure and new office symbols are as follows:

EXECUTIVE OFFICE	**AEAIM-X**
ADMINISTRATIVE SERVICES OFFICE	**AEAIM-S**
ARCHITECTURE DIVISION	**AEAIM-A**
Strategic Planning and Requirements Branch	AEAIM-A-S
Enterprise Architecture Branch	AEAIM-A-E
Policy and Standards Branch	AEAIM-A-P

C4I SUPPORT DIVISION	**AEAIM-C**
Current Operations Branch	AEAIM-C-C
Exercise Branch	AEAIM-C-E
Frequency Management Branch	AEAIM-C-F
Projects and Programs Branch	AEAIM-C-P
PUBLISHING AND RECORDS MANAGEMENT DIVISION	**AEAIM-P**
RESOURCE MANAGEMENT DIVISION	**AEAIM-R**

Operation Joint Forge and Operation Allied Force Scrolls of Appreciation

The CG, USAREUR/7A, has approved scrolls of appreciation for personnel who have taken part in recent deployments.

The Operation Joint Forge Scroll of Appreciation and the Operation Allied Force Scroll of Appreciation may be presented to military and civilian personnel who took part in or supported these operations.

Eligible personnel include those from USAREUR and other commands (for example, SHAPE, USEUCOM, USAFE), temporary change of station (TCS) augmentees from the continental United States, rear-detachment personnel, and members of affected family support groups.

The scrolls have the signature of the CG, USAREUR/7A. The first lieutenant colonel in the chain of command or supervision may countersign the scroll on the line at the lower left. Units and offices will present the scroll at an appropriate ceremony.

Commanders and staff sections should request these scrolls through their unit publications clerks. Publications clerks may order the scrolls through the *USAREUR Publications System* (UPUBS). The nomenclature for ordering--

- The Operation Joint Forge Scroll of Appreciation is US MISC Pub 19.
- The Operation Allied Force Scroll of Appreciation is US MISC Pub 21.

Tax Fraud

Merchandise intended for sale to U.S. military and civilian-component personnel is tax and duty-free and may not be sold to non-U.S. identification (ID) cardholders. The USEUCOM Customs Executive Agency uses scanner equipment to monitor documents required for importing and selling high-value items (for example, cars and motorcycles) in Germany. Customs personnel regularly detect fraudulent import permits and transfer documents, and report them to investigators.

To legally sell used property to people who do not have U.S. ID cards in Germany, U.S. personnel must--

- Have owned the items in Germany for at least 6 months before the sale.
- Use AE Form 2074 (Permit to Transfer). The value of the property must be accurately represented on the form and import duties and tax must be paid.

Personnel who lower the sale price on documents to allow a buyer to avoid tax and import duties can be charged with assisting tax evasion. Military personnel involved in assisting tax evasion can face punishment under the Uniform Code of Military Justice and by German authorities. German authorities may prosecute civilians who assist in tax evasion. Penalties include confiscation of the items involved, fines, and imprisonment, depending on the seriousness of the case.

Copier Management

Copiers in USAREUR are leased under a USAREUR-wide contract with Xerox GmbH. Only copiers required for deployment or training exercises may be purchased against Common Table of Allowances (CTA) 50-909. These copiers will be purchased using deployment funds or training funds, as appropriate, and will not be used in garrison.

New Electronic Publications

The following USAREUR publications have just been published and are available only in electronic format in the Electronic Library of USAREUR Publications and AE Forms:

- USAREUR Regulation 27-10, Military Justice, 1 February 2001
- USAREUR Regulation 215-50, Child and Youth Services Sports and Fitness Program, 9 February 2001
- USAREUR Regulation 550-50, Exercise of Foreign Criminal Jurisdiction Over United States Personnel, 31 January 2001
- USAREUR Circular 10-10-1, Directory of Key Positions, United States Army, Europe (updated on receipt of changes)

New USAREUR Command Memorandums

The following USAREUR command memorandums have been distributed as shown:

- Family Advocacy Program, AEAGA-GY (370-8916), 30 January 2001 (Dist: A)
- USAREUR Fiscal Year 2001 Retention Program, AEAGA (379-6115), 31 January 2001 (Dist: B)

Units included in the distribution should have received their copies. Proponent telephone numbers are listed after the office symbols.

USAREUR Poster Rescission

The following USAREUR poster is rescinded (the proponent staff office at HQ USAREUR/7A is shown in parentheses):

- USAREUR Poster 750-1, Telephone Numbers for Emergency Roadside Recovery Service in Germany, Italy, Belgium, Luxembourg, and the Netherlands, by Area Support Group, 1 June 1995 (ODCSLOG)

Weekly Update

At least once a week, commanders, staff principals, and supervisors are encouraged to check the Weekly Update page in the Electronic Library of USAREUR Publications and AE Forms to see if HQ USAREUR/7A has issued any new USAREUR policy.

The Weekly Update provides a list, week-by-week, of new and revised USAREUR publications and command memorandums, which are the only approved media for issuing USAREUR policy. Checking the Weekly Update page is a quick and easy way to stay informed of command policy.

How to Use This Bulletin

Appendix A
USAREUR Information Assurance Policy

USAREUR POLICY ON IT/IA WORKFORCE TRAINING

Training and Testing

A trained information technology/information assurance workforce (IT/IA workforce) is the foundation for secure computer networks. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) and USAREUR policy require special training for system administrators, network administrators and managers, IA support officers and managers, and anyone else with elevated privileges on a USAREUR network server or router, regardless of their duty assignment. This policy provides a consistent baseline of computer-network security training for the key professionals who operate and secure our computer networks.

All military, DA civilian, contractor, and local national personnel appointed to IT/IA workforce positions must be certified before being granted elevated privileges on a USAREUR network. Personnel with elevated privileges who are in USAREUR on official, temporary duty (TDY) for more than 60 days must attend training or pass the on-line Information Assurance Training Program (IATP) test before assuming IT/IA duties on a USAREUR network.

IATP Courses
The USAREUR IATP provides required information-assurance training at 12 locations in the European theater. This training meets all IA computer-training standards mandated by HQDA. Units do not have to pay for the training, but must pay for TDY costs associated with the training.

No one will be assigned to, or continue their assignment in, the IT/IA workforce, or be given elevated privileges on any portion of a USAREUR computer network unless they are certified by the DISC4 School of Technology Information Assurance Course or have attended or are scheduled to attend the USAREUR IATP.

The POC is SGM Hingtgen, USAREUR IATP Manager, DSN 381-8406/8401/8282 or e-mail: hingtgen@hq.hqusareur.army.mil. The *IATP website* also provides information on this policy.

COMPUTER-USER TEST

The USAREUR computer-user test program requires all personnel to take a computer-user test if assigned to a USAREUR or non-USAREUR organization connected to the USAREUR Army Nonsecure Internet Protocol Router Network (ANIPRNET) or the Army Secret Internet Protocol Router Network (ASIPRNET). This policy applies to all categories of employees, including military, DA civilian, contractor, and local national (LN) personnel. (The Head Works Council, USAREUR, concurs with this policy.) All USAREUR computer users must comply with this policy before being issued a network password or user identification.

The computer-user test is available in English and German on the *Information Assurance Computer-User Test webpage*. The test is open-book, multiple-choice, self-paced, and user-friendly. Users may take the test at their desks.

Before taking the test, personnel should read the USAREUR Computer-User Guide. This study guide is USAREUR Pamphlet 25-25. The German version is USAREUR Pamphlet 25-25-G. The *Information Assurance Computer-User Test webpage* provides links to the on-line versions of these study guides.

In addition to taking the test, computer users must print out the USAREUR Computer-User Agreement from the webpage and sign it. LN employees in Germany should sign the German version of this agreement. Unit system administrators will keep signed agreements in their files.

The *Information Assurance Computer-User Test webpage* provides more information on the USAREUR computer-user test program.

USAREUR POLICY ON COMPUTER ANTI-VIRUS PROTECTION

Virus attacks on computer networks worldwide are becoming more frequent and more destructive. To limit vulnerability to these attacks, HQDA requires that anti-virus signatures be updated at least every 2 weeks.

In USAREUR, anti- virus signatures on all workstations and systems will be updated at least weekly. Anti-virus signatures on exchange (e-mail) servers will be updated daily.

Computer users are responsible for updating anti-virus signatures on desktop personal computers (PCs) and laptops. An automatic, daily update pushed to individual users (automatically placed on their systems) is the preferred method for updating anti-virus signatures on PCs and laptops.

This policy applies to both classified and unclassified computer networks, but not to Uniplexed Information and Computer Systems (UNIX) or other operating systems that are not vulnerable to virus attacks.

Only the DOD-licensed Norton and McAfee anti-virus software products are authorized for use in USAREUR. The DOD site license provides Norton and McAfee anti-virus software free of charge to Army computer users. The use of any other product requires a waiver endorsed by HQ USAREUR/7A and approved by the Director of Information Systems for Command, Control, Communications, and Computers (DISC4). Waivers will not be granted without clear, strong, mission-related justification for using another anti-virus product.

The DOD site license allows DOD employees to use Norton and McAfee anti-virus software on their home computers. Contractors may not use this product on personal home computers, but may load it on company computers used for executing DOD contracts.

Current anti-virus products are available on the *Regional Computer Emergency Response Team, Europe (RCERT-E), webpage*. Users must have a ".mil" Internet protocol (IP) address to download from the RCERT-E server.

Personnel who need anti-virus software assistance may contact the RCERT-E helpdesk at 380-5232.

USAREUR POLICY ON INFORMATION ASSURANCE VULNERABILITY ALERTS

Information assurance is a commander's program. Direct command emphasis is needed to make it work.

General

Information assurance vulnerability alerts (IAVAs) are official notifications to the command that a software security vulnerability has been identified that affects one or more Army computer systems worldwide. These vulnerabilities are almost always public knowledge, and almost always involve commercial software products.

Known vulnerabilities are favorite targets of hackers, who immediately begin probing computer networks in the private and public sectors to find weak computers. Therefore, when a USAREUR command receives an IAVA, the command must quickly determine if any of its computers are affected and, if so, immediately fix them.

When DA issues an IAVA, the Deputy Chief of Staff, Operations, USAREUR, will forward it to USAREUR commands as a formal tasker. These taskers come in two forms:

- Numbered DRAGON LIGHTNING alerts, which are issued when a clear and present danger threatens the integrity, confidentiality, or availability of USAREUR data and networks, which in turn threatens USAREUR's warfighting capability.

- Numbered USAREUR IAVAs, which are issued when the threat is not as immediate or severe, but may degrade USAREUR's warfighting capability.

Responding to USAREUR IAVAs
Responses to USAREUR IAVAs will include the following information in the format provided below:

A. Number of assets affected.

B. Number of assets in compliance.

C. Number of assets with waivers.

D. Number of assets with waivers pending.

E. Number of assets not in compliance.

Suspenses Dates
Both DRAGON LIGHTNING and USAREUR IAVAs include suspense dates by which units must fix affected computers. The USAREUR standard is to meet or beat the suspense date. If an IAVA requirement cannot be met by the suspense date, the unit must contact the Army Computer Emergency Response Team Coordination Center (ACERT/ CC) through the Office of the USAREUR Information Assurance Program Manager to coordinate a plan and set a new date for compliance. The plan must--

- Provide a migration path with milestones for a security solution approved by the appropriate designated approving authority (USAREUR-command program executive officer (PEO) or program manager (PM)).

- Be forwarded to the Chief Information Officer (CIO) of the Army for approval. The CIO of the Army is the final approval authority for migration plans to implement IAVA messages.

The ACERT/CC may grant requests to extend suspense dates on behalf of the CIO of the Army. USAREUR-command PEOs and PMs, however, must acknowledge the receipt of IAVAs and report compliance with IAVA requirements.

System Compliance
All new systems that will be connected to USAREUR networks must be compliant with all IAVAs that pertain to the configuration of those systems. System administrators in USAREUR will create and locally maintain an IAVA log for each system that they manage. The logs will list all existing IAVAs

that pertain to the system and the date that each remedial action was taken on the system. If a system is reconfigured or restored after a malfunction, the log will be used to ensure that all necessary IAVA actions are reapplied. All IAVA actions reapplied and any new IAVA added at that time will be entered in the IAVA log again.

NOTE: IAVA logs are not required for individual computer workstations.

USAREUR POLICY ON INTERNET CONNECTIVITY

The security of the USAREUR information infrastructure depends on our ability to protect sensitive, unclassified information that is processed over the USAREUR Army Nonsecure Internet Protocol Router Network (ANIPRNET). This USAREUR network connects to the worldwide DOD Nonsecure Internet Protocol Router Network (NIPRNET). Protecting this network of networks requires identification, control, and management of all devices connected to it. The many interconnections between the military networks and the commercial Internet are of particular concern.

In accordance with recent guidance from DOD, the standard way for military organizations to connect to the Internet is through the ANIPRNET. Military organizations are prohibited to use a commercial Internet service provider without a waiver. Commanders of USAREUR commands (USAREUR Reg 10-5, app A) using the ANIPRNET will ensure that action is taken to terminate all connections to the Internet that do not go through the ANIPRNET.

If an ANIPRNET connection is not available, the Deputy Chief of Staff, Information Management, USAREUR, may authorize direct Internet connections, provided those computers are not on a military network.

Simultaneous connections to both the Internet and a military network open a "backdoor" into the military network. The following policy is designed to prevent backdoors unless they are absolutely necessary and then only when they are approved and configured for maximum security.

- Commanders of units with a documented requirement for simultaneous connections to both a commercial Internet service provider and the ANIPRNET must request a waiver. Waivers must be processed through the USAREUR Information Assurance Program Manager and the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) to HQDA. HQDA will validate and forward waivers to DOD for approval.

- Connections to both the Internet and a military network must be specially engineered for security applications (for example, they must have firewalls and an intrusion-detection system).

Unlike military units, educational and morale, welfare, and recreation activities are not required to connect to the Internet through the ANIPRNET. However, activities that need to maintain connectivity with a USAREUR network must make that connection with computers that are not connected directly to the Internet. Activities that use commercial Internet service providers will not be connected to the ANIPRNET with the same computers without a waiver. These connections must be specially engineered for security applications.

COMPUTER-NETWORK MISBEHAVIOR

Hacking, possessing hacker tools, or intentionally violating USAREUR policy or regulations on the use of Government computers when using USAREUR computers and networks can--

- Jeopardize the confidentiality, integrity, availability, and authentication of USAREUR information and information systems.
- Lead to adverse administrative and judicial action against the violator.

Commanders and supervisors, with help from their information technology and information assurance staff, are responsible for the discipline of USAREUR-computer-network users and operators. The information technology and information assurance staff includes the senior signal staff officer, the information management officer, system and network administrators, and information assurance managers and officers.

Limiting Damage
Personnel suspected of violating the policy on using USAREUR computers or computer networks will--

- Be suspended immediately from network access pending the results of a command inquiry.
- Have their computer accounts inactivated for the duration of the command inquiry. Passwords that these individuals know will be changed immediately.
- Be ordered not to use any USAREUR computer or network pending the results of the command inquiry.

Assessing Damage
The Regional Computer Emergency Response Team, Europe (RCERT-E), and the 202d Military Police (MP) Group, United States Army Criminal Investigation Command (USACIDC), will provide technical assistance as required to help commanders assess damage caused by the suspected computer-network misbehavior.

The RCERT-E will--

- Assess damage that may have resulted from the suspected violator's activities, particularly as they relate to the USAREUR Army Nonsecure Internet Protocol Router Network (ANIPRNET) and the Army Secret Internet Protocol Router Network (ASIPRNET).
- Serve as a liaison with the Army Computer Emergency Response Team for finding any damage or harmful activity outside the USAREUR ANIPRNET.

Computer forensic specialists from the 202d MP Group will examine the computer hard drive and other components for evidence of the suspected activity. RCERT-E personnel also will examine RCERT-E computer-activity logs.

Preserving Evidence
Computers involved in suspected violations will be removed from the network for examination by computer forensic specialists. These computers will be treated as physical evidence of a crime until released by competent MP authorities.

Determining a Course of Action
The unit information technology and information assurance staff, the RCERT-E, and the USACIDC will help the unit commander determine what violations occurred, how they happened, and what damage was caused. The commander will then take the appropriate disciplinary and administrative actions deemed necessary.

COMPUTER NETWORK MINIMIZE

Periods of increased military operating tempo (OPTEMPO) place a higher demand on our limited computer network capacity. This increased demand slows the network, which can affect mission accomplishment.

To ensure the network capacity can support our mission, the Deputy Chief of Staff, Operations (DCSOPS), USAREUR, may issue Network MINIMIZE messages during periods of increased OPTEMPO. These messages will remain in effect until they are rescinded by another DCSOPS message.

Network MINIMIZE applies only to USAREUR-operated Government computers connected to Government networks. When Network MINIMIZE is announced, units must limit their network use, particularly during peak hours of network use (0700 to 1900, Central European Time).

Examples of measures that may go in effect during Network MINIMIZE include, but are not limited to--

- Applying operations-security restrictions on the content of e-mail messages that will be sent outside of the command.
- Establishing approval authorities for e-mail messages that will be sent outside the command.
- Placing restrictions on--
    - Personal use of computer networks.
    - size of e-mail messages and attached files.
    - The use of global addresses.
    - The use of mission-related streaming audio and video.

During Network MINIMIZE, mission-essential communications, which include reasonable use of Government computer networks for morale and educational purposes, will be maintained. Personal use of Government computers will not be permitted except for the following:

- Limited morale e-mail by soldiers, civilian employees, and DOD contractors in the central region of USAREUR operations.
- Limited morale e-mail by soldiers, civilian employees, and DOD contractors in the forward area of USAREUR operations (Bosnia and Herzegovina, Kosovo, Macedonia, and other contingency locations).

- Use of unit computers by family-support groups to communicate with family members downrange, according to the time limits in the above two categories.

- Minimum-essential use of computers at Army education centers for educational purposes. This use will be restricted to offduty hours. Faculty supervision is requested.

- Minimum-essential use of unit computers for educational purposes. This use will be restricted to offduty hours and requires supervisory (GS-13, lieutenant colonel, or above) approval.

- Use of Government computers that are not connected to Government networks.

Network MINIMIZE messages will provide provisions for obtaining waivers to restrictions on network use.

PROHIBITED COMPUTER SOFTWARE

Hacker tools and other unauthorized software applications are not permitted on any USAREUR computer system except as noted below. Units and individuals who have these software applications on their USAREUR computer systems will remove them immediately.

Hacker tools--

- Are programs and applications that allow a person to break passwords, gain unauthorized access to someone else's computer system or files, or hide computer activity from auditors or intrusion-detection systems.

- Include software applications that enable criminal activity, such as generating false computer or personal identities and false credit card numbers.

- May include normal software applications if these applications are used for other than legitimate purposes.

- Can identify exploitable vulnerabilities in a computer or network peripheral (server or router) and elevate normal user permission to--

    - Give someone unauthorized access to computer resources.

    - Allow someone to read, change, or delete information that he or she normally would not be able to read, change, or delete.

Only the following individuals and organizations are permitted to have and use hacker tools and related software applications:

- Officially designated system administrators and network managers while conducting their official missions according to AR 380-19, appendix G, and AR 380-53.

- Law-enforcement and counterintelligence-computer-forensic specialists.

- Computer threat analysts of the Office of the Deputy Chief of Staff, Intelligence, HQ USAREUR/7A.
- The Regional Computer Emergency Response Team, Europe.
- The Theater Network Operations and Security Center and regional network operations and security centers, 5th Signal Command.

Other Unauthorized Software
Other software applications that may not be used on USAREUR computer systems include--

- Games.
- Personal software not authorized by the unit information assurance manager.
- Unlicensed (pirated) software.

ASSIGNING COMPUTER-USER ACCOUNTS TO FOREIGN COALITION FORCES

Among the personnel using USAREUR computers and computer networks are local national employees of, and foreign-national representatives to, the U.S. Government. The policy below applies only to foreign-national representatives to the U.S. Government.

Foreign-national representatives of Allied or Coalition partner countries (both NATO and non-NATO) --

- May be provided limited-access user accounts on unclassified USAREUR computer networks.
- Must sign a computer-user agreement before being given an account.
- May use accounts only for communicating with the U.S. Coalition command structure under which they fall. This use must be consistent with the mission of the Coalition command and with the guidance issued by the U.S. commander responsible for the computer network.

E-mail addresses of foreign-national representatives must include a prefix that identifies the accountholder's country. This prefix must appear before the accountholder's name (for example, uk.smith@tf.army.mil or german.schmidt@tf. army.mil). User accounts given to foreign-national representatives will be separated or limited so as not to have the privileges associated with army.mil domain rights.

If a foreign-national representative needs network access for a valid military mission, the access requirement must be validated by the Deputy Chief of Staff, Information Management, USAREUR; the Deputy Chief of Staff, Operations, USAREUR; and the USAREUR Information Assurance Program Manager before access is provided. The computer network will be configured for foreign-national representatives so that it provides only e-mail service and, if Internet access is required to accomplish a military mission, only the minimum Internet access required for the mission.

USAREUR policy on the appropriate use of USAREUR computer networks and on limited personal use of U.S. Government computers also applies to foreign-national representatives. Those who misuse

USAREUR computer networks will lose access to them, and financial reimbursement for any monetary liability will be requested from the sending country if permitted by applicable international agreements.

USAREUR POLICY ON COALITION NETWORKS

Computer networks established for combined (Coalition) joint task force missions should operate at security and access levels that will best support the personnel involved in the missions.

A Coalition Secret network, in which foreign-national representatives in the Coalition provide information by "air gap" (transferring information from one system to another by using a diskette or compact disk), is the most useful computer-network architecture for joint task forces. Joint task force operations centers that use Coalition Secret networks avoid problems that arise from using U.S. Only Secret networks, to which foreign-national representatives do not have access.

Most information on Coalition networks pertains to the Coalition and may be shared with foreign-national representatives based on a mission-driven "need to know." National information that supports multinational efforts may be shared based on national rules. U.S. personnel who share national information must follow National Disclosure Policy (AR 380-10).

Information provided to Coalition networks must pass through U.S. national information centers (NICs). A U.S. NIC will be established as the authorized terminus for classified and unclassified, U.S. Only computer networks and other telecommunications traffic. NATO commands are encouraged to establish a NATO information center to serve as a terminus for NATO traffic when the Coalition includes non-NATO members. Information from NICs is screened for clearance to Coalition networks and sent to these networks electronically through an approved, one-way electronic filter or by air gap.

Under no circumstances will non-U.S. citizens be--

- Given a computer-user account on any U.S. classified network for any reason.
- Assigned to work in any area (office, tent, open bay) where U.S. Only classified information is being processed.

USAREUR policy on foreign-national access governs access to unclassified networks by Coalition foreign-national representatives.

USAREUR IA COUNCIL OF COLONELS

The mission of the USAREUR Information Assurance Council of Colonels (IA CoC) is to provide commandwide awareness of the USAREUR Information Assurance Program and commandwide input to information assurance policy, procedures, and priorities in USAREUR. The USAREUR IA CoC will include--

- The USAREUR Information Assurance Program Manager (IAPM) (chairperson).
- The Assistant Deputy Chief of Staff, Personnel, USAREUR.
- The Assistant Deputy Chief of Staff, Intelligence, USAREUR.

- The Assistant Deputy Chief of Staff, Operations, USAREUR.
- The Chief, Operations Division, Office of the Deputy Chief of Staff, Operations, HQ USAREUR/7A.
- The Assistant Deputy Chief of Staff, Logistics (Operations), USAREUR.
- The Assistant Deputy Chief of Staff, Resource Management, USAREUR.
- The Assistant Deputy Chief of Staff, Information Management, USAREUR.
- The Chief, Public Affairs, USAREUR.
- The Judge Advocate, USAREUR (or deputy if the deputy is a colonel).
- The Provost Marshal, USAREUR.
- The Deputy Chief of Staff, Operations, 5th Signal Command.
- One representative from each USAREUR command (USAREUR Reg 10-5, app A).
- One representative from each major tenant command.

The USAREUR IA CoC will meet at least semiannually at a time and place suitable to the CoC and to the matters being discussed. The USAREUR IAPM will coordinate the meeting agenda with council members, direct the meetings, and provide a written summary of actions taken and taskers that arise during each meeting.

Attendance by noncouncil members at council meetings will be at the discretion of the USAREUR IAPM and the council members and be based on available seating, the need for subject-matter experts, and the parties involved.

USAREUR POLICY ON COMMERCIAL INTERNET CHAT

Commercial Internet-chat tools present an unacceptable risk to the integrity, availability, and confidentially of USAREUR data and data networks. Commercial-chat features and capabilities are not permitted on the USAREUR Army Nonsecure Internet Protocol Router Network (ANIPRNET). USAREUR computer users who have a legitimate military need for commercial-chat features that cannot be met by *Army Knowledge Online* or another DOD-sponsored chat or e-mail forum should contact the USAREUR Information Assurance Program Manager to request access.

INFORMATION ASSURANCE EMERGENCY AND INCIDENT PROCEDURES

A threat to any networked computer anywhere in DOD is a threat to DOD computer systems worldwide. In response to this type of threat, HQDA has instituted a 4-hour reporting requirement for IA emergencies. The standing operating procedures (SOPs) of the offices involved provide specific reporting procedures.

- An IA emergency is an ongoing security vulnerability that has the potential for major damage to data or major degradation of automation services that would adversely affect the USAREUR warfighting mission. An IA emergency requires USAREUR and HQDA notification within 4 hours.

    - Actual or suspected intrusions in USAREUR and significant computer-network vulnerabilities are reported to the Watch Officer, Office of the Deputy Chief of Staff, Operations, HQ USAREUR/7A. The Watch Officer will notify specific USAREUR commanders by telephone and send them a follow-up executive summary by e-mail. The officer will follow procedures in the Watch Officer SOP.

    - When a situation has the potential for commandwide information or system damage, the USAREUR Information Assurance Program Manager may declare an IA emergency alert, code word DRAGON LIGHTNING. DRAGON LIGHTNING alerts are processed by the USAREUR Emergency Action Center for rapid, commandwide notification. Notification will be by telephone (conference call) and follow-up flash message.

- An IA incident is an ongoing security vulnerability that does not meet the criteria of an IA emergency but requires prompt correction. An IA incident normally will be limited to duty-hour and duty-day notification.

- Routine information (for example, software-vulnerability notices, new viruses, suspicious Internet protocol addresses) will be reported daily during the workweek in the Current Regional Computer Emergency Response Team, Europe (RCERT-E), Operations Activity Report. The reporting cutoff time is 1700 Central European Time (CET). Incidents must be reported to the Watch Officer by 1800 CET.

USAREUR POLICY ON WEBSITE SECURITY

Organizations with websites must take steps to limit exposing webservers to risk.

Public Websites
All public websites (those intended for unrestricted access) will be moved to servers managed by the Office of the Chief, Public Affairs (OCPA), HQ USAREUR/7A. The OCPA will coordinate and announce a timeline for moving websites. These servers will remain accessible from Internet protocol (IP) addresses in Europe and North America.

Private Websites
Private websites (those limited to a specific domain (DOD, Army, USAREUR, or other defined group)) will remain on organizational webservers, and security measures will be taken locally and at the network perimeter. To comply with Message, HQDA, SAIS-ZA, 101256Z May 00, subject: Public Key Enabling of Private Web Servers, all private Army webservers in USAREUR must operate secure socket layer (SSL) protocol using a Class 3 Public Key Certificate issued by the DOD Public Key Infrastructure (PKI). The *Regional Computer Emergency Response Team, Europe, webpage* provides information on implementing SSLs on private webservers.

Additional local security measures, such as password protection or limiting the range of authorized IP addresses, are at the discretion of each organization. After all public websites have moved to the OCPA server, perimeter security will be increased to further limit the range of IP addresses authorized access

to the network.

USAREUR POLICY ON REMOTE ACCESS TO E-MAILBOXES

If remote access to an e-mailbox on an unclassified Microsoft Exchange server is required, the only authorized means of gaining access to the mailbox is by connecting through one of the following:

- A modem using a terminal-server access card.
- A DOD ".mil" network using an authorized Microsoft Exchange client or Internet Explorer if using Outlook Web Access.

When using a remote-access server, the mailbox access must be password-controlled according to USAREUR password policy.

POP3 E-MAIL

Post Office Protocol 3 (POP3) e-mail is quick and user-friendly, but is unsecure in its regular format. The use of POP3 e-mail poses a threat to USAREUR computer networks because it transmits the user's identification and password unencrypted. POP3 e-mail is enabled by default when installing Exchange Server 5.0 or higher.

POP3 e-mail on unclassified Microsoft Exchange servers has been prohibited in USAREUR since 1 August 2000. It is on the USAREUR list of unauthorized network services and is blocked from the Army Nonsecure Internet Protocol Router Network (ANIPRNET).

POP3 e-mail may, however, be encrypted using a secure socket layer (SSL). The SSL diverts e-mail from the default port that is blocked by the USAREUR security router to another port that uses an SSL. System administrators either will disable POP3 e-mail at the site and server level for all Microsoft Exchange servers under their control or install an SSL that encrypts e-mail.

Waivers to this policy will be considered under exceptional circumstances. The Deputy Chief of Staff, Information Management, USAREUR, is the waiver-approval authority.

This bulletin is an official publication of HQ USAREUR/7A